Dell EqualLogic PS Series iSCSI Storage Arrays With Microsoft Windows Server Failover Clusters Hardware Installation and Troubleshooting Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Information in this publication is subject to change without notice.

© 2012 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the Dell logo, Dell Precision™ , OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

2012 - 02

Rev. A05

Contents

Notes, Cautions, and Warnings....2

1 Introduction....5
- Cluster Solution....5
- Cluster Hardware Requirements....6
  - Cluster Nodes....6
  - Cluster Storage....6
  - Network Configuration Recommendations....8
- Supported Cluster Configurations....9
  - iSCSI SAN-Attached Cluster....9
- Other Documents You May Need....9

2 Cluster Hardware Cabling....11
- Mouse, Keyboard, And Monitor Cabling Information....11
- Power Supplies Cabling Information....11
- Cluster Cabling Information For Public And Private Networks....12
  - For Public Network....13
  - For Private Network....13
  - NIC Teaming....14
- Storage Array(s) Cabling Information....14
  - Cabling The Storage For Your iSCSI SAN-Attached Cluster....14

3 Preparing Your Systems For Clustering....27
- Configuring A Cluster....27
- Installation Overview....28
  - Additional Information For Installing iSCSI NICs....28
  - Host Integration Tools....28
  - Installing The Microsoft iSCSI Software Initiator....33
  - Modifying The Registry Settings....34
  - Configuration Overview Of Shared Storage Arrays....34
- Advanced Storage Features....37
  - Snapshots....38
  - Volumes....39
  - Replication....40
  - Volume Collections....41
  - Thin Provisioning....41
- Installation And Configuration Of A Failover Cluster....41

4 Troubleshooting....43

5 Cluster Data Form....47

6 iSCSI Configuration Worksheet....49

1

Introduction

A Dell Failover Cluster combines specific hardware and software components to provide enhanced availability for applications and services that run on your cluster. A Failover Cluster reduces the possibility of any single point of failure within the system that can cause the clustered applications or services to become unavailable. It is recommended that you use redundant components like servers, storage power supplies, connections between the nodes and the storage array(s), and connections to client systems or other servers in a multi-tier enterprise application architecture in your cluster.

This document provides information and specific configuration tasks that enable you to configure your Failover Cluster with Dell EqualLogic PS Series Internet Small Computer System Interface (iSCSI) storage array(s).

For more information on deploying your cluster with Microsoft Windows Server 2003 operating systems, see the *Dell Failover Clusters with Microsoft Windows Server 2003 Installation and Troubleshooting Guide* at **support.dell.com/manuals**.

For more information on deploying your cluster with Windows Server 2008 operating systems, see the *Dell Failover Clusters with Microsoft Windows Server 2008 Installation and Troubleshooting Guide* at **support.dell.com/manuals**.

For a list of supported operating systems, hardware components, and driver or firmware versions for your Failover Cluster, see the *Dell Cluster Configuration Support Matrices* at **dell.com/ha**.

Cluster Solution

Your cluster supports a minimum of two nodes to a maximum of either eight nodes (with Windows Server 2003 operating systems) or sixteen nodes (with Windows Server 2008 operating systems) and provides the following features:

- Gigabit and 10 Gigabit Ethernet iSCSI technologies
- High availability of resources to network clients
- Redundant paths to the shared storage
- Failure recovery for applications and services
- Flexible maintenance capabilities, allowing you to repair, maintain, or upgrade a node or storage array without taking the entire cluster offline

The iSCSI protocol encapsulates iSCSI frames that include commands, data, and status into Transmission Control Protocol/Internet Protocol (TCP/IP) packets to be transported over Ethernet networks. The iSCSI frames are sent between the Microsoft iSCSI Initiator that resides in the host and the iSCSI target, which is a storage device. Implementing iSCSI in a cluster provides the following advantages:

Geographic distribution	Wider coverage of Ethernet technology allows cluster nodes and storage arrays to be located in different sites.
Low cost for availability	Redundant connections provide multiple data paths that are available through inexpensive TCP/IP network components.
Connectivity	A single technology for connection of storage array(s), cluster nodes, and clients.

Cluster Hardware Requirements

Your cluster requires the following hardware components:

- Cluster nodes
- Cluster storage

Cluster Nodes

The following section lists the hardware requirements for the cluster nodes.

Component	Minimum Requirement
Cluster nodes	A minimum of two identical Dell PowerEdge systems are required. The maximum number of nodes that are supported depend on the variant of the Windows Server operating system used in your cluster.
RAM	The variant of the Windows Server operating system that is installed on your cluster nodes determines the minimum required amount of system RAM.
Microsoft iSCSI Software Initiator	Help initialize the array(s), configure and manage host access to the array(s). The Host Integration Tools also includes Microsoft iSCSI Software Initiator.
Network Interface Cards (NICs) for iSCSI access	Two iSCSI NICs or two iSCSI NIC ports per node. Configure the NICs on separate PCI buses to improve availability and performance. TCP/IP Offload Engine (TOE) NICs are also supported for iSCSI traffic.
NICs (public and private networks)	At least two NICs: one NIC for the public network and another NIC for the private network. **NOTE:** If your configuration requires more than two iSCSI NIC ports, contact Dell Services. **NOTE:** It is recommended that the NICs on each public network are identical and that the NICs on each private network are identical.
Internal disk controller	One controller connected to at least two internal hard drives for each node. Use any supported Redundant Array of Independent Disks (RAID) controller or disk controller. Two hard drives are required for mirroring (RAID 1) and at least three hard drives are required for disk striping with parity (RAID 5). **NOTE:** It is highly recommended that you use hardware-based RAID or software-based disk-fault tolerance for the internal drives.

Cluster Storage

Cluster nodes can share access to external storage array(s). However, only one of the nodes can own any volume in the external storage array(s) at any time. Microsoft Cluster Services (MSCS) controls which node has access to each volume.

The following section lists the configuration requirements for the storage system, cluster nodes, and stand-alone systems connected to the storage system.

Cluster Storage Requirements

Hardware Components	Requirement
Storage system	One or more Dell EqualLogic PS Series groups. Each Dell EqualLogic PS5000/PS5500/ PS6000/PS6010/PS6100/PS6110/PS6500/PS6510 group supports up to sixteen storage arrays (members) and each PS4000/PS4100/PS4110 group supports up to two storage arrays. For specific storage array requirements, see Dell EqualLogic PS Series Storage Array Requirements
Storage interconnect	All nodes must be attached to one or more storage arrays through an iSCSI SAN.
Multiple clusters and stand-alone systems	Can share one or more supported storage arrays.

A Dell EqualLogic PS series storage array includes redundant, hot-swappable disks, fans, power supplies, and control modules. A failure in one of these components does not cause the array to be offline. The failed component can be replaced without bringing the storage array down.

The following section lists hardware requirements for the Dell EqualLogic PS series storage arrays.

Dell EqualLogic PS Series Storage Array Requirements

Dell EqualLogic Array Model	Minimum Required Features
PS4000 — PS4000E/PS4000X/PS4000XV	Redundant control modules
PS4100 — PS4100E/PS4100X/PS4100XV	
PS4110 — PS4110E/PS4110X/PS4110XV	
PS5000 — PS5000E/PS5000X/PS5000XV	
PS5500 — PS5500E	
PS6000 — PS6000E/PS6000X/PS6000XV/PS6000S	
PS6010 — PS6010E/PS6010X/PS6010XV/PS6010S/PS6010XVS	
PS6100 — PS6100E/PS6100X/PS6100XV/PS6100S/PS6100XS	
PS6110 — PS6110E/PS6110X/PS6110XV/PS6110S/PS6110XS	
PS6500 — PS6500E/PS6500X	
PS6510 — PS6510E/PS6510X	

NOTE: Ensure that the storage array(s) are running a supported firmware version. For specific firmware version requirements, see the *Dell Cluster Configuration Support Matrices* at **dell.com/ha**.

NICs Dedicated To iSCSI

The NIC controlled by the iSCSI software initiator acts as an I/O adapter to connect the expansion bus of the system and the storage array(s). Failover Cluster solutions that are configured with the EqualLogic PS Series storage arrays require two iSCSI NICs or NIC ports in each PowerEdge system. This provides redundant paths and load balance of the I/O data transfer to or from the storage array(s).

Network Switches Dedicated To iSCSI

The Gigabit or 10 Gigabit switches for iSCSI access function as regular network switches and provide dedicated interconnection between the nodes and the storage array(s).

Network Configuration Recommendations

It is recommended that you follow the guidelines in this section. In addition to these guidelines, all the usual rules for proper network configuration apply to group members.

Recommendation	Description
Network connections between array(s) and hosts	Connect array(s) and hosts to a switched network and ensure that all network connections between hosts and array(s) are Gigabit or 10 Gigabit Ethernet.
A reliable and adequately sized network link for replication	For effective and predictable replication, ensure that the network link between the primary and secondary groups is reliable and provides sufficient bandwidth for copying data.
No Spanning-Tree Protocol (STP) functionality on switch ports that connect end nodes	Do not use STP on switch ports that connect end nodes (iSCSI initiators or storage array network interfaces). However, if you want to use STP or Rapid Spanning-Tree Protocol (RSTP) (preferable to STP), enable the port settings available on some switches that let the port immediately transition into STP forwarding state upon link up. This functionality can reduce network interruptions that occur when devices restart and should only be enabled on switch ports that connect end nodes. **NOTE:** It is recommended that you use Spanning-Tree and trunking for multi-cable connections between switches.
Connectivity between switches	The iSCSI switches must be connected together. Use stacking ports or port trunking to create a high-bandwidth link between the switches. If a single non-stacking link is used, it can become the bottle-neck and negatively affect the performance of the storage system.
Enable Flow Control on switches and NICs	Enable Flow Control on each switch port and NIC that handles iSCSI traffic. Dell EqualLogic PS Series arrays correctly respond to Flow Control.
Disable Unicast storm control on switches	Disable Unicast storm control on each switch that handles iSCSI traffic, if the switch provides this feature. However, the use of broadcast and multicast storm control is encouraged on switches.
Enable Jumbo Frames on switches and NICs	Enable Jumbo Frames on each switch and NIC that handles iSCSI traffic to obtain performance benefit and ensure consistent behavior.
Disable iSCSI Optimization on switches	Disable iSCSI Optimization, if the switch provides this feature, to avoid blocking internal communication between the array members.

Supported Cluster Configurations

iSCSI SAN-Attached Cluster

In an iSCSI switch-attached cluster, all the nodes are attached to a single storage array or to multiple storage arrays through redundant iSCSI SANs for high-availability. iSCSI SAN-attached clusters provide superior configuration flexibility, expandability, and performance.

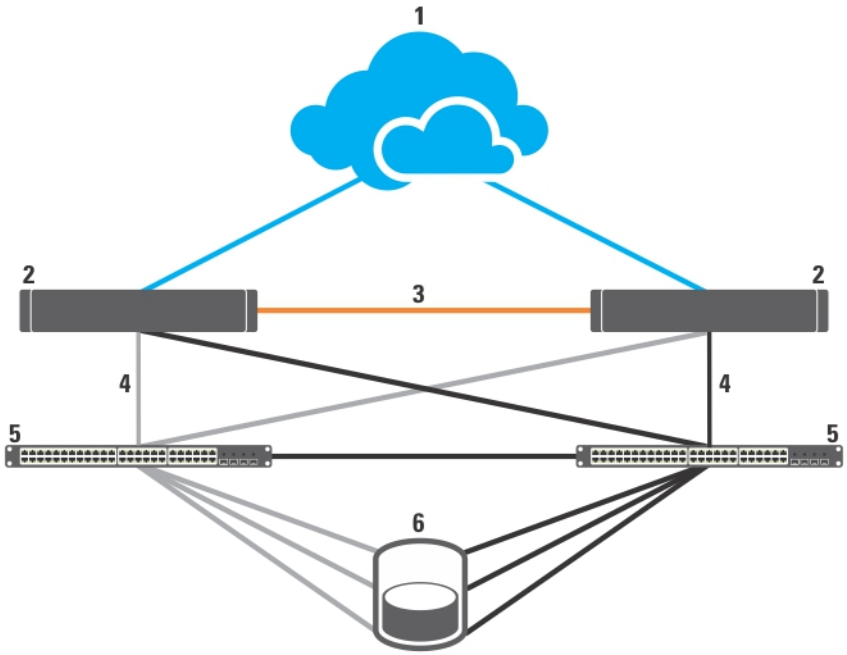


Figure 1. iSCSI SAN-Attached Cluster

1. public network
2. cluster nodes
3. private network
4. iSCSI connections
5. Gigabit or 10 Gigabit Ethernet switches
6. storage system

Other Documents You May Need

CAUTION: For important safety and regulatory information, see the safety information that is shipped with your system. Warranty information may be included within this document or as a separate document.

The following documentation is available at **support.dell.com/manuals** and **equallogic.com**:

- The *Rack Installation Guide* included with your rack solution describes how to install your system into a rack.
- The *Getting Started Guide* provides an overview of initially setting up your system.
- The *Dell Failover Clusters with Microsoft Windows Server 2003 Installation and Troubleshooting Guide* provides more information on deploying your cluster with the Windows Server 2003 operating system.
- The *Dell Failover Clusters with Microsoft Windows Server 2008 Installation and Troubleshooting Guide* provides more information on deploying your cluster with the Windows Server 2008 operating system.

- The *Dell Cluster Configuration Support Matrices* provides a list of supported operating systems, hardware components, and driver or firmware versions for your Failover Cluster.
- Operating system documentation describes how to install (if necessary), configure, and use the operating system software.
- Documentation for any hardware and software components you purchased separately provides information to configure and install those options.
- The Dell PowerVault tape library documentation provides information for installing, troubleshooting, and upgrading the tape library.
- Dell EqualLogic documentation:
  - Release Notes — Provides the latest information about the Dell EqualLogic PS Series arrays and/or Host Integration Tools.
  - QuickStart — Describes how to set up the array hardware and create a Dell EqualLogic PS Series group.
  - Group Administration — Describes how to use the Group Manager graphical user interface (GUI) to manage a Dell EqualLogic PS Series group.
  - CLI Reference — Describes how to use the Group Manager command line interface (CLI) to manage a Dell EqualLogic PS Series group and individual arrays.
  - Hardware Maintenance — Provides information about maintaining the array hardware.
  - Host Integration Tools Installation and User Guide — Provides information on creating and expanding the Dell EqualLogic PS Series groups, configuring multipath I/O, performing manual transfer replication, and backing up and restoring data.
  - *Host Integration Tools EqualLogic Auto-Snapshot Manager/Microsoft Edition User Guide* — Provides information for creating and managing copies of storage objects (such as volumes or databases) located on the Dell EqualLogic PS series groups.
  - SAN HeadQuarters User Guide — Provides centralized monitoring, historical performance trending, and event reporting for multiple PS series groups.
  - Online Help — In the Group Manager GUI, expand **Tools** in the far left panel and then click **Online Help** for help on both the GUI and the CLI.
- Release notes or readme files may be included to provide last-minute updates to the system or documentation, or advanced technical reference material intended for experienced users or technicians.

2

Cluster Hardware Cabling

This section provides information on cluster hardware cabling.

Mouse, Keyboard, And Monitor Cabling Information

When installing a cluster configuration in a rack, you must include a switch box to connect the mouse, keyboard, and monitor to the nodes. For instructions on cabling the connections of each node to the switch box, see the documentation included with your rack.

Power Supplies Cabling Information

See the documentation for each component in your cluster solution to ensure that the specific power requirements are satisfied.

The following guidelines are recommended to protect your cluster solution from power-related failures:

- For cluster nodes and storage arrays with multiple power supplies, plug each power supply into a separate AC circuit.
- Use uninterruptible power supplies (UPS).
- For some environments, consider having backup generators and power from separate electrical substations.

The following figures illustrate recommended methods for power cabling a cluster solution consisting of two Dell PowerEdge systems and one storage array. To ensure redundancy, the primary power supplies of all the components are grouped into one or two circuits and the redundant power supplies are grouped into a different circuit.

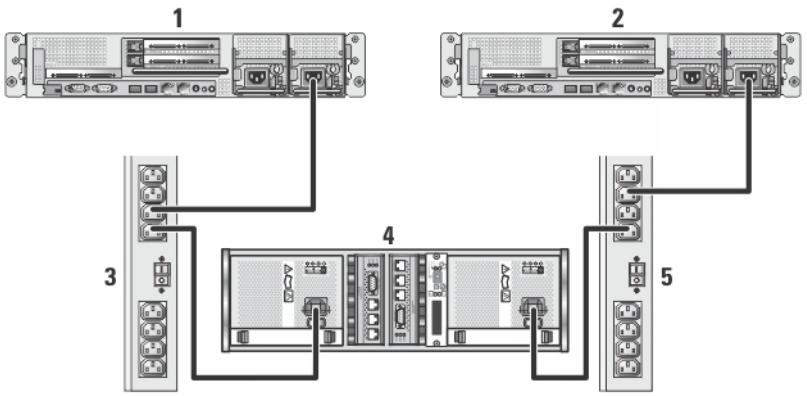


Figure 2. Power Cabling Example With One Power Supply in PowerEdge Systems

1. cluster node 1
2. cluster node 2
3. primary power supplies on one AC power strip
4. EqualLogic PS series storage array

5. redundant power supplies on one AC power strip

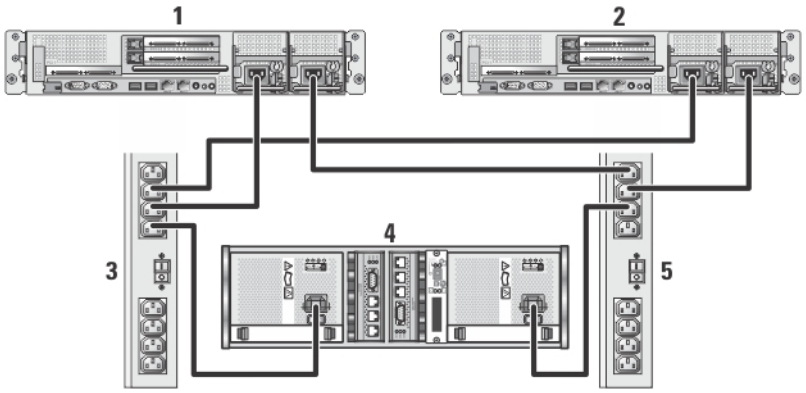


Figure 3. Power Cabling Example With Two Power Supplies in the PowerEdge Systems

1. cluster node 1
2. cluster node 2
3. primary power supplies on one AC power strip
4. EqualLogic PS series storage array
5. redundant power supplies on one AC power strip

Cluster Cabling Information For Public And Private Networks

The network adapters in the cluster nodes provide at least two network connections for each node.

The following section describes the network connections.

Network Connection	Description
Public network	– All connections to the client LAN. – At least one public network must be configured for both client access and cluster communications.
Private network	A dedicated connection for sharing cluster health and status information only.

The following figure shows an example of cabling in which dedicated network adapters in each node are connected to each other (for the private network) and the remaining network adapters are connected to the public network.

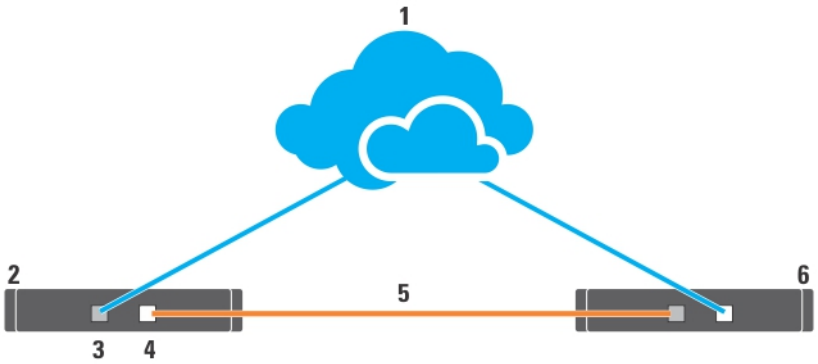


Figure 4. Example of Network Cabling Connection

1. public network
2. cluster node 1
3. public network adapter
4. private network adapter
5. private network
6. cluster node 2

For Public Network

Any network adapter supported by a system running TCP/IP may be used to connect to the public network segments. You can install additional network adapters to support additional public network segments or to provide redundancy in the event of a faulty primary network adapter or switch port.

For Private Network

The private network connection to the nodes is provided by a different network adapter in each node. This network is used for intra-cluster communications. The following table describes the two possible private network configurations.

Method	Hardware Components	Connection
Network switch	Gigabit or 10 Gigabit Ethernet network adapters and switches	Depending on the hardware, connect the CAT5e CAT6, CAT6a, or CAT7 cables, the multi-mode optical cables with Local Connectors (LCs), or the twinax cables from the network adapters in the nodes to a switch.
Point-to-Point (two-node clusters only)	Copper Gigabit network adapters with RJ-45 connectors	Connect a CAT5e or better (CAT6, CAT6a, or CAT7) Ethernet cable between the network adapters in both nodes.
	Copper 10 Gigabit Ethernet network adapters with RJ-45 connectors	Connect a CAT6 or better (CAT6a or CAT7) Ethernet cable between the network adapters in the nodes.
	Copper 10 Gigabit Ethernet network adapters with SFP+ connectors	Connect a twinax cable between the network adapters in both nodes.

Method	Hardware Components	Connection
	Optical Gigabit or 10 Gigabit Ethernet network adapters with LC connectors	Connect a multi-mode optical cable between the network adapters in both nodes.

Dual-Port Network Adapters Usage

You can configure your cluster to use the public network as a failover for private network communications. If dual-port network adapters are used, do not use both ports simultaneously to support both the public and private networks.

NIC Teaming

NIC teaming combines two or more NICs to provide load balancing and fault tolerance. Your cluster supports NIC teaming, but only for the public network; NIC teaming is not supported for the private network or an iSCSI network.

NOTE: Use the same brand of NICs in a team, and do not mix brands of teaming drivers.

Storage Array(s) Cabling Information

This section provides information for connecting your cluster to one or more storage arrays.

Connect the cables between the iSCSI switches and configure the iSCSI switches. For more information see, Network Configuration Recommendations.

Connect the iSCSI ports from the servers and array(s) to the Gigabit switches, using proper network cables.

For Gigabit iSCSI ports with RJ-45 connectors: use CAT5e or better (CAT6, CAT6a, or CAT7)

For 10 Gigabit iSCSI ports:

- With RJ-45 connectors: use CAT6 or better (CAT6a or CAT7)
- With LC connectors: use fiber optic cable acceptable for 10GBASE-SR
- With SFP+ connectors: use twinax cable

Cabling The Storage For Your iSCSI SAN-Attached Cluster

An iSCSI SAN-attached cluster is a cluster configuration where all cluster nodes are attached to a single storage array or to multiple storage arrays using redundant iSCSI switches.

The following figures show examples of a two-node iSCSI SAN-attached cluster and a sixteen-node iSCSI SAN-attached cluster.

Similar cabling concepts can be applied to clusters that contain a different number of nodes.

NOTE: The connections listed in this section are a representative of one proven method of ensuring redundancy in the connections between the cluster nodes and the storage array(s). Other methods that achieve the same type of redundant connectivity may be acceptable.

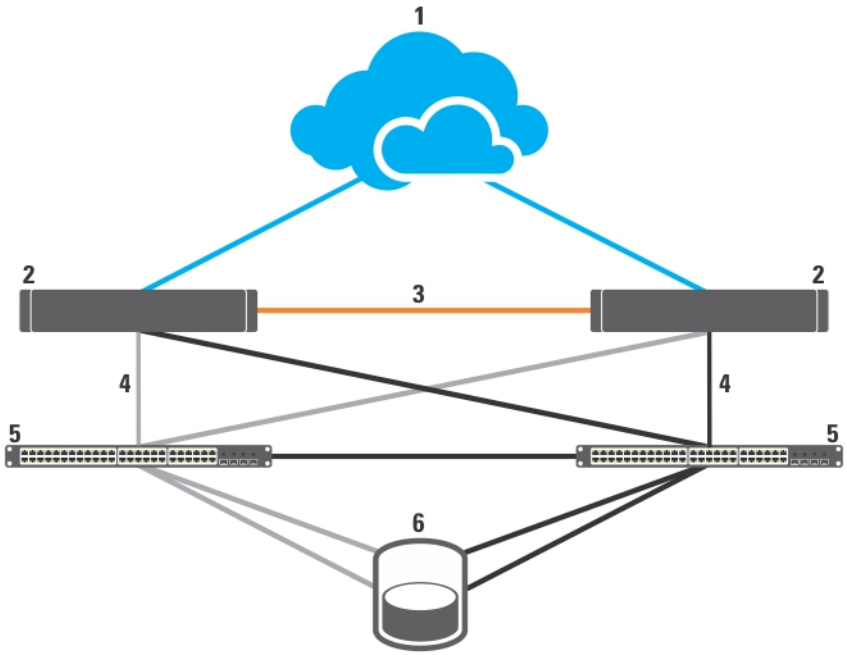


Figure 5. Two-Node iSCSI SAN-Attached Cluster

1. public network
2. cluster node
3. private network
4. iSCSI connections
5. Gigabit or 10 Gigabit Ethernet switches
6. storage system

Gigabit NICs can access the 10 Gigabit iSCSI ports on the EqualLogic PS4110/PS6010/PS6110/PS6510 storage systems if any one of the following conditions exist:

- The switch supports both Gigabit and 10 Gigabit Ethernet.
- The servers connected to a Gigabit Ethernet switch are cascaded to the 10 Gigabit Ethernet that is attached to the storage system.

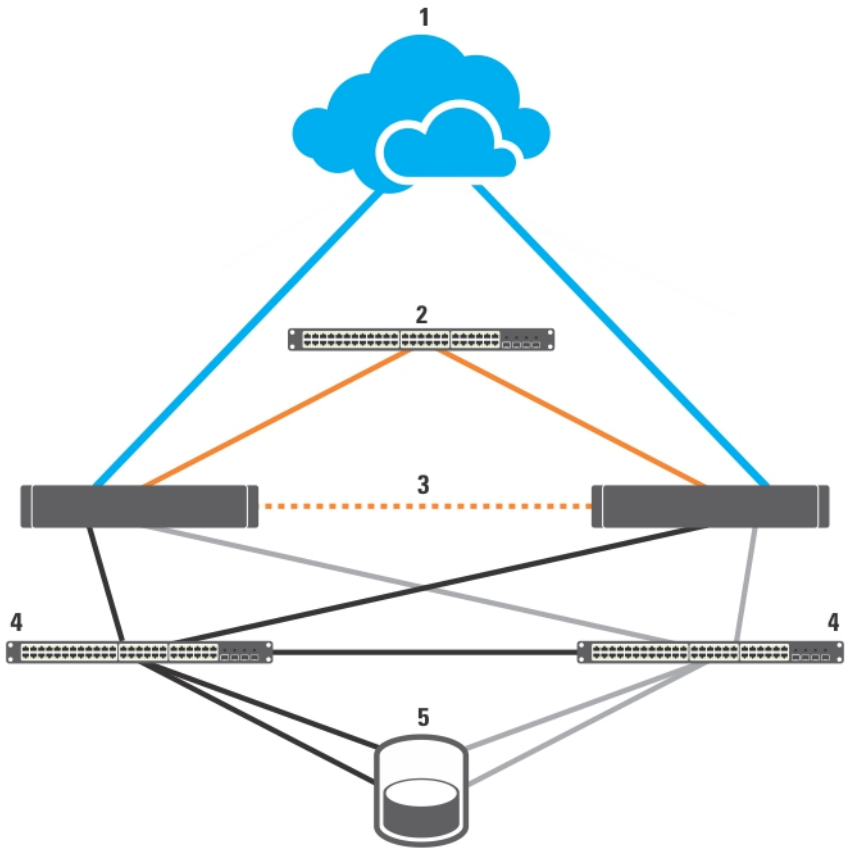


Figure 6. Sixteen-Node iSCSI SAN-Attached Cluster

1. public network
2. private network
3. cluster nodes (2-16)
4. Gigabit or 10 Gigabit Ethernet switches
5. storage system

Cabling One iSCSI SAN-Attached Cluster To The Dell EqualLogic PS Series Storage Array(s)

1. Connect cluster node 1 to the iSCSI switches:
   a) Connect a network cable from iSCSI NIC 0 (or NIC port 0) to the network switch 0.
   b) Connect a network cable from iSCSI NIC 1 (or NIC port 1) to the network switch 1.
2. Repeat step 1 for each cluster node.
3. Connect the Dell EqualLogic PS Series storage array(s) to the iSCSI switches.

   For more information on cabling the specific storage arrays, see the following sections.

Cabling The Dell EqualLogic PS4110/PS6110 Storage Arrays

1. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 0.
2. Connect a network cable from the network switch 1 to Ethernet 0 on the control module 1.
3. Repeat steps 1 and 2 to connect the additional Dell EqualLogic PS4110/PS6110 storage array(s) to the iSCSI switches.

NOTE: You can use only one of the two 10 Gb Ethernet ports on each control module at a time. With the 10GBASE-T port (left Ethernet 0 port), use CAT6 or better cable. With the SFP+ port (right Ethernet 0 port), use fiber optic cable acceptable for 10GBASE-SR or twinax cable.

For more information, see the figures below.

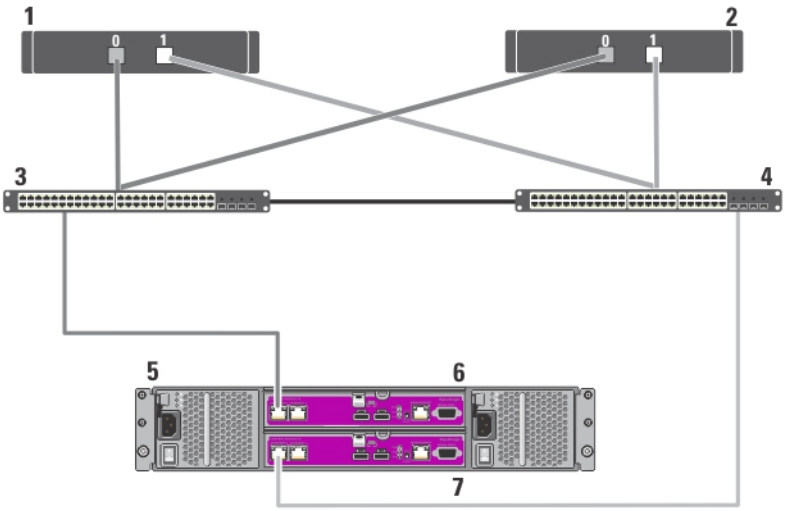


Figure 7. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS4110 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS4110 storage system
6. control module 0
7. control module 1

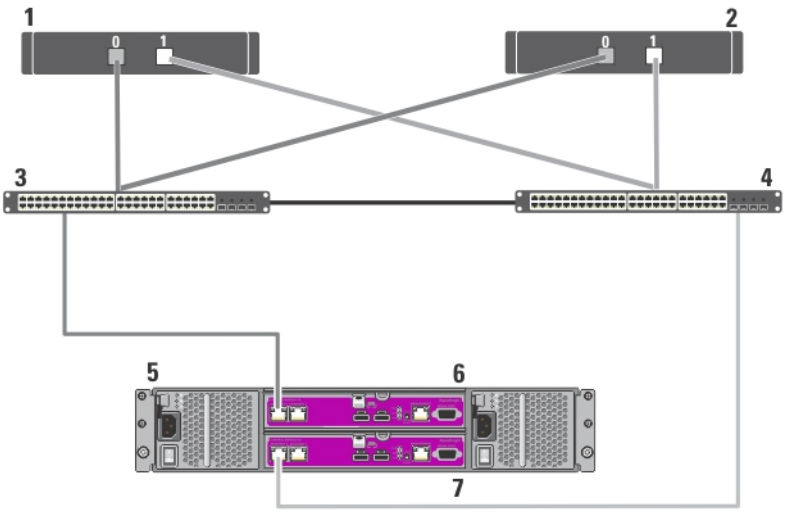


Figure 8. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS6110 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS6110 storage system
6. control module 0
7. control module 1

Cabling The Dell EqualLogic PS4000/PS4100/PS6010/PS6510 Storage Arrays

1. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 1.
2. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 0.
3. Connect a network cable from the network switch 1 to Ethernet 1 on the control module 1.
4. Connect a network cable from the network switch 1 to Ethernet 1 on the control module 0.
5. Repeat steps 1 to 4 to connect the additional Dell EqualLogic PS4000/PS4100/PS6010/PS6510 storage array(s) to the iSCSI switches.

NOTE: For PS4100 storage array, having all 4 cables in steps 1 through 4 provides highest level of cable redundancy. It works fine with only 2 cables. You can skip either step 1 or 2, and either step 3 or 4.

For more information, see the figures below.

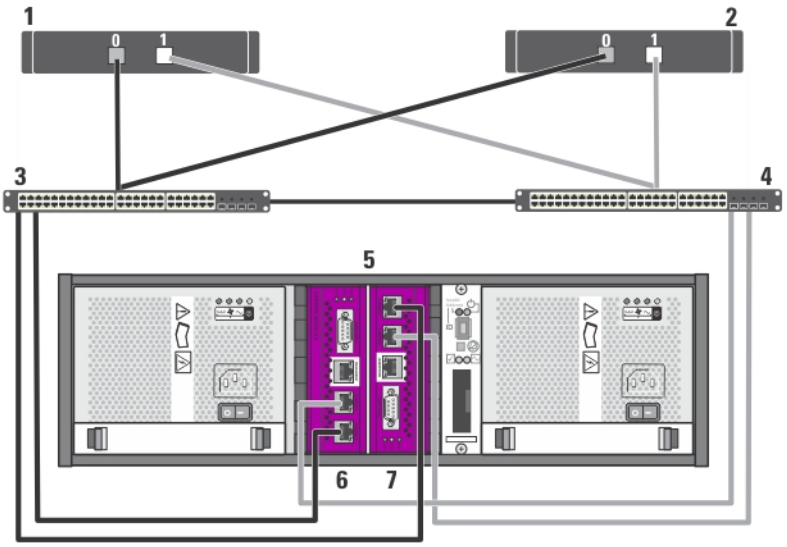


Figure 9. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS4000 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS4000 storage system
6. control module 1
7. control module 0

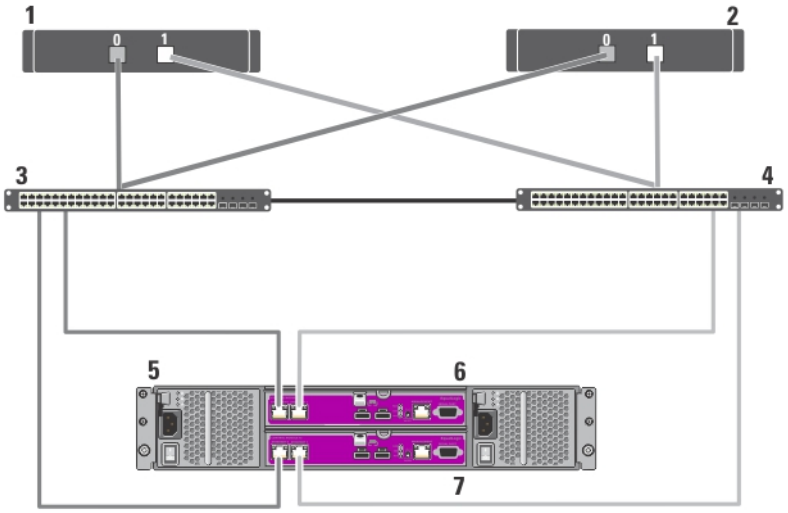


Figure 10. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS4100 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS4100 storage system
6. control module 0
7. control module 1

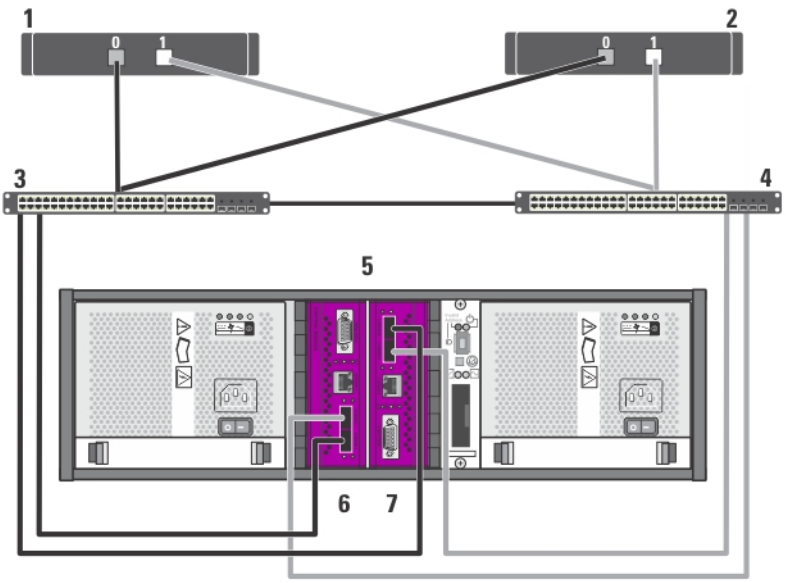


Figure 11. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS6010 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS6010 storage system
6. control module 1

7. control module 0

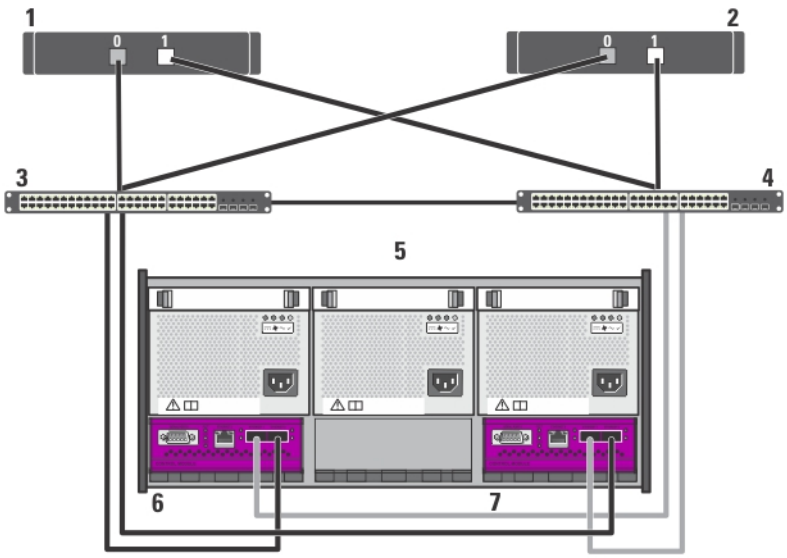


Figure 12. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS6510 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS6510 storage system
6. control module 1
7. control module 0

Cabling The Dell EqualLogic PS5000/PS5500 Storage Arrays

1. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 1.
2. Connect a network cable from the network switch 0 to Ethernet 1 on the control module 1.
3. Connect a network cable from the network switch 1 to Ethernet 2 on the control module 1.
4. Connect a network cable from the network switch 1 to Ethernet 0 on the control module 0.
5. Connect a network cable from the network switch 1 to Ethernet 1 on the control module 0.
6. Connect a network cable from the network switch 0 to Ethernet 2 on the control module 0.
7. Repeat steps 1 to 6 to connect the additional Dell EqualLogic PS5000/PS5500 storage array(s) to the iSCSI switches. For more information, see the figures below.

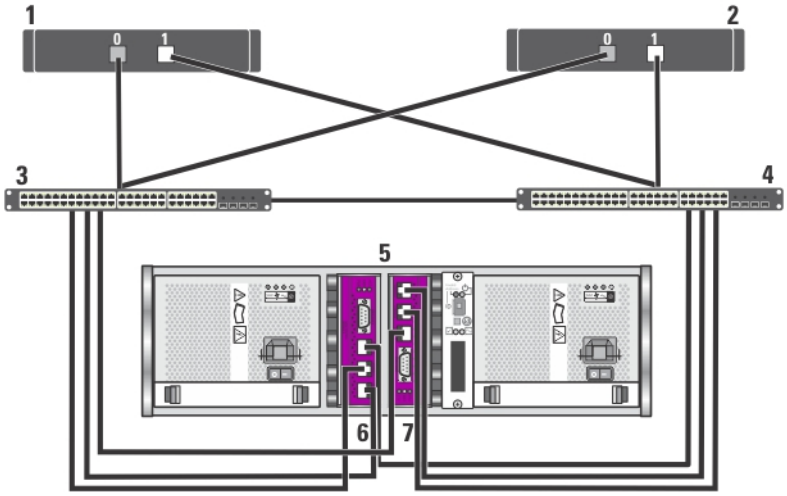


Figure 13. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS5000 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS5000 storage system
6. control module 1
7. control module 0

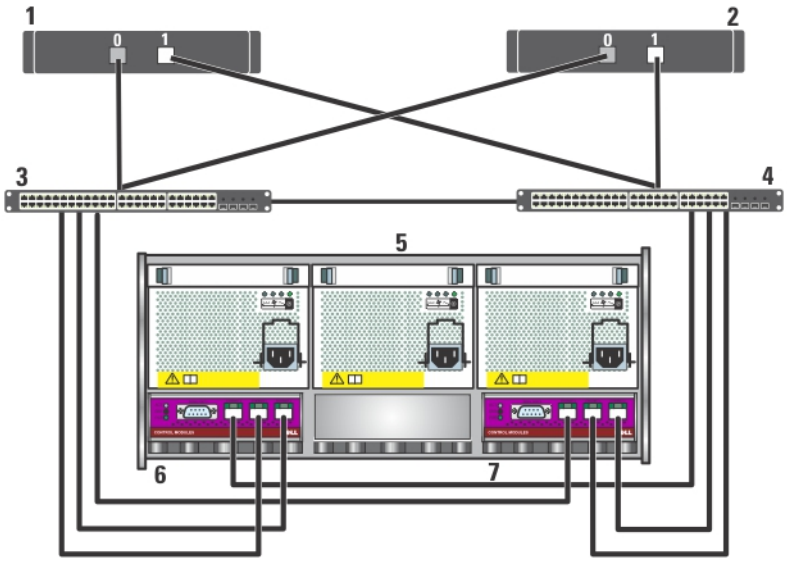


Figure 14. Cabling an iSCSI SAN-attached cluster to a Dell EqualLogic PS5500 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS5500 storage system
6. control module 1
7. control module 0

Cabling The Dell EqualLogic PS6000/PS6100/PS6500 Storage Arrays

1. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 1.
2. Connect a network cable from the network switch 0 to Ethernet 1 on the control module 1.
3. Connect a network cable from the network switch 1 to Ethernet 2 on the control module 1.
4. Connect a network cable from the network switch 1 to Ethernet 3 on the control module 1.
5. Connect a network cable from the network switch 1 to Ethernet 0 on the control module 0.
6. Connect a network cable from the network switch 1 to Ethernet 1 on the control module 0.
7. Connect a network cable from the network switch 0 to Ethernet 2 on the control module 0.
8. Connect a network cable from the network switch 0 to Ethernet 3 on the control module 0.
9. Repeat steps 1 to 8 to connect the additional Dell EqualLogic PS6000/PS6100/PS6500 storage array(s) to the iSCSI switches.

NOTE: For PS6100 storage array, having all eight cables in steps 1 through 4 provides highest level of cable redundancy. It works fine with only four cables. You can skip either step 1 or 5, either step 2 or 6, either step 3 or 7, and either step 4 or 8.

For more information, see the figures below.

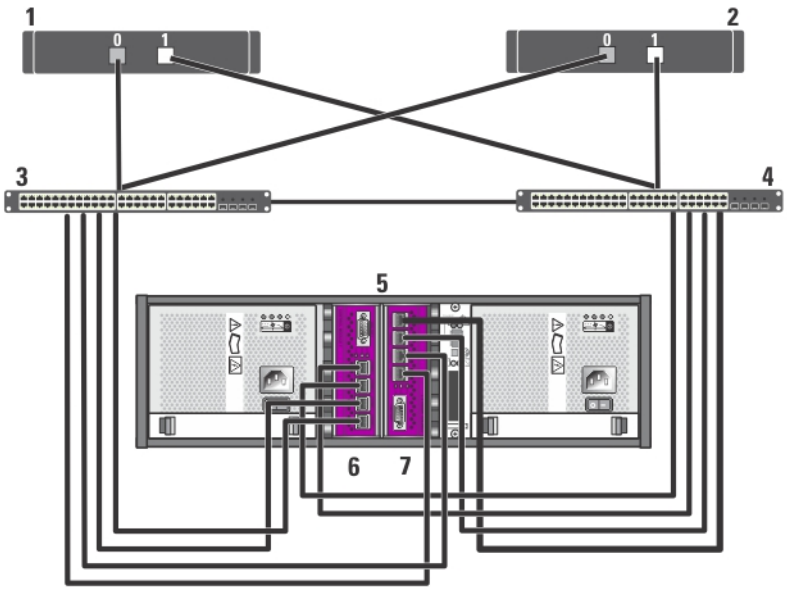


Figure 15. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS6000 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS6000 storage system
6. control module 1
7. control module 0

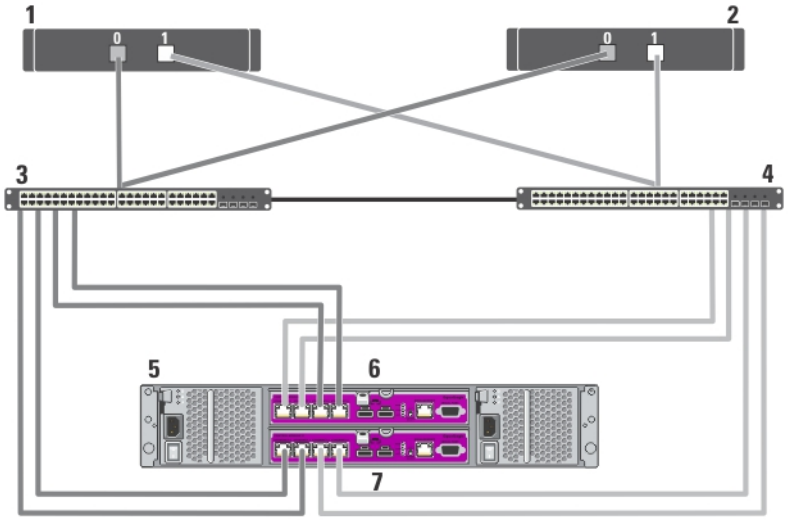


Figure 16. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS6100 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1
5. Dell EqualLogic PS6100 storage system
6. control module 0
7. control module 1

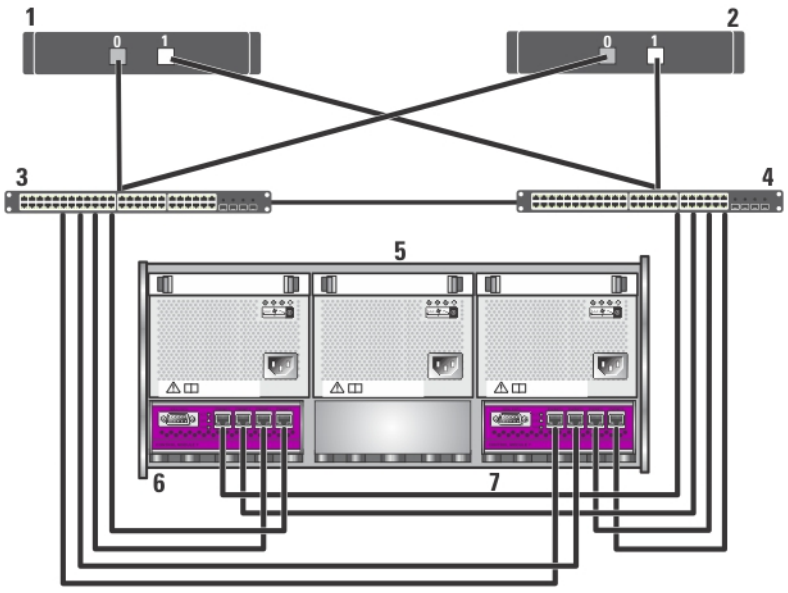


Figure 17. Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS6500 Storage Array

1. cluster node 1
2. cluster node 2
3. switch 0
4. switch 1

5. Dell EqualLogic PS6500 storage system
6. control module 1
7. control module 0

Cabling Multiple iSCSI SAN-Attached Clusters To The Dell EqualLogic PS Series Storage Array(s)

To cable multiple clusters to the storage array(s), connect the cluster nodes to the appropriate iSCSI switches and then connect the iSCSI switches to the control modules on the Dell EqualLogic PS Series storage array(s).

NOTE: The following procedure uses the figure titled Cabling an iSCSI SAN-Attached Cluster to a Dell EqualLogic PS5000 Storage Array as an example for cabling additional clusters.

1. In the first cluster, connect cluster node 1 to the iSCSI switches.
   a) Connect a network cable from iSCSI NIC 0 (or NIC port 0) to the network switch 0.
   b) Connect a network cable from iSCSI NIC 1 (or NIC port 1) to the network switch 1.
2. Repeat step 1 for each node.
3. For each additional cluster, repeat step 1 and step 2.
4. Connect the Dell EqualLogic PS Series storage array(s) to the iSCSI switches.

   For more information on cabling the specific storage arrays, see the following sections.

Cabling Multiple iSCSI SAN-Attached Clusters For Dell EqualLogic PS4110/PS6110 Storage Arrays

1. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 0.
2. Connect a network cable from the network switch 1 to Ethernet 0 on the control module 1.
3. Repeat steps 1 and 2 to connect the additional Dell EqualLogic PS4110/PS6110 storage array(s) to the iSCSI switches.

NOTE: You can use only one of the two 10 Gb Ethernet ports on each control module at a time. With the 10GBASE-T port (left Ethernet 0 port), use CAT6 or better cable. With the SFP+ port (right Ethernet 0 port), use fiber optic cable acceptable for 10GBASE-SR or twinax cable.

Cabling Multiple iSCSI SAN-Attached Clusters For Dell EqualLogic PS4000/PS4100/PS6010/PS6510 Storage Arrays

1. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 1.
2. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 0.
3. Connect a network cable from the network switch 1 to Ethernet 1 on the control module 1.
4. Connect a network cable from the network switch 1 to Ethernet 1 on the control module 0.
5. Repeat steps 1 to 4 to connect the additional Dell EqualLogic PS4000/PS4100/PS6010/PS6510 storage array(s) to the iSCSI switches.

NOTE: For PS4100 storage array, having all 4 cables in steps 1 through 4 provides highest level of cable redundancy. It works fine with only 2 cables. You can skip either step 1 or 2, and either step 3 or 4.

Cabling Multiple iSCSI SAN-Attached Clusters For Dell EqualLogic PS5000/PS5500 Storage Arrays

1. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 1.
2. Connect a network cable from the network switch 0 to Ethernet 1 on the control module 1.
3. Connect a network cable from the network switch 1 to Ethernet 2 on the control module 1.
4. Connect a network cable from the network switch 1 to Ethernet 0 on the control module 0.
5. Connect a network cable from the network switch 1 to Ethernet 1 on the control module 0.
6. Connect a network cable from the network switch 0 to Ethernet 2 on the control module 0.
7. Repeat steps 1 to 6 to connect the additional Dell EqualLogic PS5000/PS5500 storage array(s) to the iSCSI switches.

Cabling Multiple iSCSI SAN-Attached Clusters For Dell EqualLogic PS6000/PS6100/PS6500 Storage Arrays

1. Connect a network cable from the network switch 0 to Ethernet 0 on the control module 1.
2. Connect a network cable from the network switch 0 to Ethernet 1 on the control module 1.
3. Connect a network cable from the network switch 1 to Ethernet 2 on the control module 1.
4. Connect a network cable from the network switch 1 to Ethernet 3 on the control module 1.
5. Connect a network cable from the network switch 1 to Ethernet 0 on the control module 0.
6. Connect a network cable from the network switch 1 to Ethernet 1 on the control module 0.
7. Connect a network cable from the network switch 0 to Ethernet 2 on the control module 0.
8. Connect a network cable from the network switch 0 to Ethernet 3 on the control module 0.
9. Repeat steps 1 to 8 to connect the additional Dell EqualLogic PS6000/PS6100/PS6500 storage array(s) to the iSCSI switches.

NOTE: For PS6100 storage array, having all eight cables in steps 1 through 4 provides highest level of cable redundancy. It works fine with only four cables. You can skip either step 1 or 5, either step 2 or 6, either step 3 or 7, and either step 4 or 8.

Obtaining More Information

For more information on configuring the cluster components, see the storage and tape backup documentation at **support.dell.com/manuals**.

3

Preparing Your Systems For Clustering

CAUTION: Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that came with the product.

Configuring A Cluster

The following instructions give you an overview on how to configure a cluster.

1. Ensure that your site can handle the power requirements of the cluster. Contact your sales representative for information about your region's power requirements.
2. Install the systems, the shared storage array(s), and the interconnect switches (for example, in an equipment rack) and ensure that all the components are turned on.
3. Deploy the operating system (including any relevant service packs and hotfixes) and network adapter drivers on each cluster node. Depending on the deployment method that is used, it may be necessary to provide a network connection to successfully complete this step.

NOTE: To help in planning and deployment of your cluster, record the relevant cluster configuration information in the Cluster Data Form and the iSCSI configuration information in the iSCSI Configuration Worksheet.

4. Establish the physical network topology and the TCP/IP settings for network adapters on each cluster node to provide access to the cluster public and private networks.
5. Configure each cluster node as a member in the same Microsoft Active Directory Domain.

NOTE: You can configure the cluster nodes as Domain Controllers. For more information, see Selecting a Domain Model in the *Dell Failover Clusters with Microsoft Windows Server 2003 Installation and Troubleshooting Guide* or *Dell Failover Clusters with Microsoft Windows Server 2008 Installation and Troubleshooting Guide* at **support.dell.com/manuals**.

6. Establish the physical storage topology and any required storage array(s) settings to provide connectivity between the storage array(s) and the systems that you are configuring as cluster nodes. Configure the storage array(s) as described in your storage array documentation.
7. Use storage array management tools to create at least one volume and then assign the volume(s) to all cluster nodes. The volume is used as a cluster Quorum disk for Microsoft Windows Server 2003 Failover Cluster or as a Witness disk for Windows Server 2008 Failover Cluster.
8. Select one of the systems and form a new Failover Cluster by configuring the cluster name, cluster management IP, and quorum resource. For more information, see Preparing Your Systems For Clustering.

NOTE: For Failover Clusters configured with Windows Server 2008, run the **Cluster Validation Wizard** to ensure that your system is ready to form the cluster.

9. Join the remaining node(s) to the Failover Cluster. For more information, see Preparing Your Systems For Clustering.
10. Configure roles for cluster networks. Take any network interfaces that are used for iSCSI storage (or for other purposes outside the cluster) out of the control of the cluster.
11. Test the failover capabilities of your new cluster.

NOTE: For Failover Clusters configured with Windows Server 2008, you can also use the **Cluster Validation Wizard**.

12. Configure highly-available applications and services on your Failover Cluster. Depending on your configuration, this may also require providing additional volumes to the cluster or creating new cluster resource groups. Test the failover capabilities of the new resources.
13. Configure client systems to access the highly-available applications and services that are hosted on your Failover Cluster.

Installation Overview

Each cluster node in the Failover Cluster must have the same release, edition, service pack, and processor architecture of the Windows Server operating system installed. For example, all nodes in your cluster may be configured with the Windows Server 2003 R2, Enterprise x64 Edition operating system. If the operating system varies among nodes, it may not be possible to configure a Failover Cluster successfully. It is recommended that you establish server roles prior to configuring a Failover Cluster, depending on the operating system configured on your cluster.

For a list of Dell PowerEdge systems, iSCSI NICs, supported list of operating system variants, and specific driver and firmware revisions, see the *Dell Cluster Configuration Support Matrices* at **dell.com/ha**.

The following sub-sections describe steps that enable you to establish communication between the cluster nodes and your shared Dell EqualLogic PS series storage array(s), and to present disks from the storage array(s) to the cluster:

- Installing the iSCSI NICs
- Installing the Host Integration Tools
- Installing the Microsoft iSCSI Software Initiator
- Modifying the Registry Settings
- Configuring the Shared Storage Array(s)
- Installing and Configuring a Failover Cluster

Additional Information For Installing iSCSI NICs

- It is recommended that you install the latest and compatible service packs or hotfixes of the NIC driver.
- For optimal performance benefit, it is recommended that you enable Flow Control and Jumbo Frames on each NIC and switch that handles iSCSI traffic.
- For information about supported NICs and drivers, see the *Dell Cluster Configuration Support Matrices* at **dell.com/ha**.

Host Integration Tools

The Host Integration Tools include:

Remote Setup Wizard	Enables you to initialize an EqualLogic PS Series storage array and to set up and configure access to a Dell EqualLogic PS Series group. The wizard also enables you to configure multipath I/O on the Windows Server 2003 and Windows Server 2008 operating system.
Multipath I/O Device Specific Module (DSM)	Enables you to configure multiple redundant network paths between a system running the Windows operating system and EqualLogic PS Series group volumes for high availability and high performance.
Auto-Snapshot Manager/Microsoft Edition (ASM/ME)	Enables you to implement Microsoft Volume Snapshot Service (VSS) to create snapshots, clones, and replicas to provide point-in-time protection of critical data for supported applications, including Microsoft SQL Server, Exchange Server, Hyper-V, and NTFS file shares. The Auto-Snapshot Manager is a VSS Requestor and includes a VSS Provider.

NOTE: For more information on using ASM in the cluster, see the *Host Integration Tools EqualLogic Auto-Snapshot Manager/Microsoft Edition User Guide* at **support.dell.com/manuals**.

NOTE: ASM is supported in the cluster environment with Host Integration Tools version 3.2 or later.

- VDS Provider — Enables you to use the Microsoft Virtual Disk Service (VDS) and Microsoft Storage Manager for SANs to create and manage volumes in a EqualLogic PS Series group.
- Microsoft iSCSI Software Initiator — Includes the iSCSI port driver, Initiator Service, and Software Initiator to help connect to iSCSI devices via the Windows TCP/IP stack using NICs. For information about using the Microsoft iSCSI Software Initiator, see the documentation at **microsoft.com**.

Installing The Host Integration Tools

1. Obtain the Host Integration Tools kit from the Technical Support website or the *Host Integration Tools* media shipped with a EqualLogic PS Series array.
2. Start the installation by downloading the kit from the website or inserting the *EqualLogic Host Integration Tools for Microsoft Windows* media in the system.
3. Click **View Documentation** in the installer screen to display the *Host Integration Tools User Guide*. It is highly recommended that you read the *User Guide* and the *Host Integration Tools Release Notes* before continuing with the installation.
4. For Host Integration Tools version 3.1.1, run **setup.exe**. For Host Integration Tools version 3.2 or later, run **setup.exe -cluster**.
5. Specify information about the installation when prompted. You can choose the **Typical** installation, which installs all the tools supported by the operating system, or you can choose the **Custom** installation, which allows you to select the tools you want to install.

Running The Remote Setup Wizard

The **Remote Setup Wizard** simplifies Dell EqualLogic PS Series group (SAN) and Windows system setup.

After you install the Host Integration Tools, you can choose to launch the Remote Setup Wizard automatically, or you can run it later using the following step:

1. Click **Start Programs → Equallogic → Remote Setup Wizard**
2. Select the task to perform:
   - Initialize an array (and create or expand a group).
   - Configure the system to access a PS Series SAN.
   - Configure multipath I/O between a system and PS Series group volumes.

EqualLogic PS Series Arrays And Groups

Using the Remote Setup Wizard, you can initialize a EqualLogic PS Series array and create an EqualLogic PS Series group with the array as the first member. In addition, the wizard sets up system access to the group, configuring the group IP address as the iSCSI target discovery address and enabling Microsoft service (VSS or VDS) access to the group through Challenge-Handshake Authentication Protocol (CHAP) authentication.

Before you initialize an array and create a group, gather information about the array configuration and the group configuration. For more information, see the tables below. The **Remote Setup Wizard** prompts you for the array and group configuration information.

Array Configuration

Prompt	Description
Member name	Unique name (up to 63 numbers, letters, or hyphens) used to identify the array in the group. The first character must be a letter or number.

Prompt	Description
IP address	Network address for the Ethernet 0 network interface.
Netmask	Combines with the IP address to identify the subnet on which the Ethernet 0 network interface resides.
Default gateway	Network address for the device used to connect subnets and forward network traffic beyond the local network. A default gateway is used to allow the Ethernet 0 network interface to communicate outside the local network (for example, to allow access to volumes from computers outside the local network). **NOTE:** The default gateway must be on the same subnet as the Ethernet 0 network interface.
RAID policy	RAID policy configured on the first member of the group: – RAID 10 — Striping on top of multiple RAID 1 (mirrored) sets, with one or two spare disks. – RAID 10 provides good performance for random writes, in addition to the highest availability. – RAID 50 — Striping on top of multiple RAID 5 (distributed-parity) sets, with one or two spare disks. RAID 50 provides a good balance of performance (especially for sequential writes), availability, and capacity. – RAID 5 — One RAID 5 set, with one spare disk. RAID 5 is similar to RAID 50, with more capacity (two additional disks) but lower availability and performance. – RAID 6 — Of the total number of disks installed in the array, two disks are used for parity and one disk is a spare. The remainder are data disks.

Group Configuration

Prompt	Description
Group name	Unique name (up to 63 letters, numbers, or hyphens) used to identify the group. The first character must be a letter or number.
Group IP address	Network address for the group. The group IP address is used for group administration and for discovery of the resources (i.e. volumes). Access to the resources is through a physical port IP address.
Password for managing group membership	Password required when adding members to the group. The password must have 3 to 16 alphanumeric characters and is case-sensitive.
Password for the default group administration account	Password that overrides the factory-set password (grpadmin) for the default grpadmin account. The password must have 3 to 16 alphanumeric characters and is case-sensitive.
Microsoft service user name and password	CHAP user name and password used to enable Microsoft service (VSS or VDS) access to the group. The user name must have between 3 and 54 alphanumeric characters. The password must have 12 to 16 alphanumeric characters, and is case-sensitive. Microsoft services running on a computer must be allowed access to the group in order to create VSS snapshots in the group or use VDS.

Initializing An Array And Creating A Group

1. Start the **Remote Setup Wizard**.
2. In the **Welcome** dialog box, select **Initialize a PS Series array**, and click **Next**.
   A list of arrays is displayed in the **Select an Array to Initialize** dialog box.
3. Select an array and click **Details** to display details, including the serial number and MAC address.
4. Select the array you want to initialize and click **Next**.

5. Enter the array configuration in the **Initialize an Array** dialog box. For more information, see Array Configuration.
6. Click a field name link to display help on the field. In addition, choose the option to create a new group. Then, click **Next**.
7. Enter the group configuration in the **Creating a Group** dialog box and then, click **Next**. For more information, see Group Configuration.

   A message is displayed when the array has been initialized.
8. Click **OK**.
9. When the **Finish** dialog box is displayed, you can do one of the following:

   – Click **View Log** to display a summary of the configuration.
   – Click **Next** to initialize another array and add it to the group.
   – Click **Finish** to complete the configuration and exit the wizard.

   After you click **Finish**, the wizard:

   – Configures the group IP address as an iSCSI discovery address on the computer.
   – Stores the CHAP user name and password that allows Microsoft services (VDS or VSS) access to the group on the computer.
   – Creates a corresponding VSS/VDS access control record and local CHAP account in the group.

NOTE: To view the VSS/VDS access control record, click **Group Configuration** → **VSS/VDS**.

NOTE: To display the local CHAP account in the group, click **Group Configuration** → **iSCSI** tab.

After you create a group, use the Group Manager GUI or CLI to create and manage volumes.

Initializing An Array And Expanding A Group

Using the **Remote Setup Wizard**, you can initialize a Dell EqualLogic PS Series array and add the array to an existing group. In addition, the wizard configures the group IP address as an iSCSI discovery address on the computer.

Before you initialize an array and expand a group, make sure you have the following information:

- The array configuration details, as described in the Array Configuration table.
- Group name, IP address, and membership password, as described in the Group Configuration table.

Follow the steps below to initialize an array and expand an existing group:

1. Start the **Remote Setup Wizard**.
2. In the **Welcome** dialog box, select **Initialize a PS Series array**, and click **Next**.
3. Select the array you want to initialize and click **Next**.
4. Enter the array network configuration in the **Initialize an Array** dialog box.

   For more information, see the Array Configuration table.
5. Select the array that must be added to an existing group and click **Next**.
6. Enter the group name a, IP address, and the membership password in the **Joining a Group** dialog box, and click **Next**.

   When the initialized array successfully joins the group, the following message is displayed:

   ```
   Member Successfully Added to Group.
   ```
7. Click **Yes** to open the Group Manager GUI to configure a RAID policy for the new member, or click **No** to configure RAID later.
8. When the **Finish** dialog box is displayed, you can:

   – Click **View Log** to display a summary of the configuration.
   – Click **Next** to initialize another array and add it to the group.

– Click **Finish** to complete the configuration and exit the wizard.

When you exit the wizard, it configures the group IP address as an iSCSI discovery address on the computer, if not already present.

After you join a group, you can use the Group Manager GUI or CLI to create and manage volumes.

Computer Access To A Group

You can use the **Remote Setup Wizard** to enable Windows computer access to a Dell EqualLogic PS Series group. You can also use the wizard to modify existing group access information on a computer (for example, if the group IP address changed).

NOTE: When you create a group using the **Remote Setup Wizard**, computer access to the group is automatically configured. This section applies only if you used **Remote Setup Wizard** on a different computer to create the group, or created the group through the serial cable instead of **Remote Setup Wizard**.

When you use the **Remote Setup Wizard** to enable computer access to a group, the wizard performs the following:

1. Configures the group IP address as an iSCSI target discovery address. This enables the computer to discover volumes and snapshots (iSCSI targets) in the group.
2. Stores the CHAP user name and password that allow Microsoft services (VDS or VSS) access to the group.

Enabling Computer Access To A Group

To enable computer access to a group or modify existing group access information:

1. Obtain the following information:
   - Name and IP address of the group.
   - CHAP user name and password already configured in the group for Microsoft service (VSS or VDS) access to the group.

NOTE: To use the Group Manager GUI to display the VSS/VDS access control record, click **Group Configuration → VSS/VDS** .

NOTE: To display the local CHAP account in the group, click **Group Configuration → iSCSI**.

2. Launch the **Remote Setup Wizard**.
3. In the **Remote Setup Wizard - Welcome** window, select **Configure this computer to access a PS Series SAN**, and click **Next**.
4. In the Configuring Group Access dialog box, you can:
   - Click **Add Group** to add a group that the computer can access.
   - Select a group and click **Modify Group** to modify existing group access.
5. In the **Add or Modify Group Information** dialog box:
   a) Specify or modify the group name and IP address, as needed.
   b) If the group is configured to allow Microsoft service (VDS or VSS) access to the group through CHAP, specify the CHAP user name and password that matches the VSS/VDS access control record and local CHAP account already configured in the group.
   c) If the PS Series group is configured to restrict discovery based on CHAP credentials, click the check box next to **Use CHAP credentials for iSCSI discovery**.
   d) Click **Save**.
6. In the **Configuring Group Access** dialog box, click **Finish**.

Configuring Multipath I/O Between A Computer And A Group

To configure multipath I/O between a computer and a group:

1. Start the **Remote Setup Wizard**.
2. In the **Welcome** dialog box, select **Configure MPIO settings for this computer**, and click **Next**.

   The **Configure MPIO Settings** dialog box is displayed.
3. By default, all host adapters on all subnets that are accessible by the PS Series group are configured for multipath I/O. If you want to exclude a subnet, move it from the left panel to the right panel. Also, select whether you want to enable balancing the I/O load across the adapters.

NOTE: To exclude a specific IP address on a subnet, manually edit the registry variables. For more information, see the *Host Integration Tools Release Notes*.

4. Click **Finish** to complete the multipath I/O configuration. Click **Back** to make changes, if required.

Changes to the list of included or excluded subnets are effective immediately for new connections, while changes to existing connections may take several minutes.

Configuring Firewall To Allow ICMP Echo Requests

If you are using Windows firewall on your system, configure your firewall to allow Internet Control Message Protocol (ICMP) echo requests for ICMPv4.

To configure your firewall:

NOTE: This procedure is applicable for Windows Server 2008 only. For other versions of Windows operating systems, see the documentation that is shipped with your system.

1. Click **Start** → **Administrative Tools** → **Windows Firewall with Advanced Security**.
2. Click **Inbound Rules** in the **Main** pane and **New Rule** in the **Actions**pane.
3. Check **Custom** and click **Next**.
4. Check **All programs** and click **Next**.
5. Select **ICMPv4** from the **Protocol type** drop-down menu.
6. Click **Customize Internet Control Message Protocol (ICMP)** settings.
7. Check **Specific ICMP types** and then check **Echo** request.
8. Click **OK** and then, **Next**.
9. Specify the local and remote IP addresses. For each type (local or remote), check **Any IP Address** or **These IP addresses**. If you check the latter, you must also type in one or more IP addresses. Click **Next** when you have finished specifying IP addresses.
10. Check **Allow the connection**, and click **Next**. Look for the options under the label: **When does this rule apply?**
11. Check one of the following options:
    - Domain
    - Private
    - Public
12. Click **Next**.
13. Enter a name for this rule and an optional description.
14. Click **Finish**.

Installing The Microsoft iSCSI Software Initiator

This section is applicable to those Windows Server 2003 operating systems where the Host Integration Tools are not used to install the initiator. The Host Integration Tools include a version of the Microsoft iSCSI Software Initiator. For information on the supported iSCSI Software Initiator version, see the *Dell Cluster Configuration Support Matrices* at **dell.com/ha**. If the version in the Host Integration Tools is not listed in the Support Matrix, download and install the Microsoft iSCSI Software Initiator using the following steps:

1. Use a web browser and go to the Microsoft Download Center website at **microsoft.com/downloads**.
2. Search for *iscsi initiator*.
3. Select and download the latest supported initiator software and related documentation for your operating system.
4. Double-click the executable file. The installation wizard launches.
5. In the **Welcome** screen, click **Next**.
6. In the following screens, select the **Initiator Service**, **Software Initiator**, and **Microsoft MPIO Multipathing Support for iSCSI** options.
7. Click **Next** to continue with the installation.
8. Read and accept the license agreement and click **Next** to install the software.
9. In the completion screen, click **b** to complete the installation.
10. Select the **Do not restart now** option to reboot the system after modifying the registry settings in the section Modifying the Registry Settings.

Modifying The Registry Settings

After you have installed the **Host Integration Tools** kit version 3.1.1 or later, the utility **EqlSetupUtil.exe** is stored in the directory **\EqualLogic\bin**.

To configure the registry values, perform the following steps for each cluster host:

1. To configure the registry values, perform the following steps for each cluster host:
2. Go to the **EqualLogic\bin** directory. The default location is **c:\Program Files\EqualLogic\bin**.
3. For a Windows Server 2003 host, run *EqlSetupUtil.exe -PRKey <PR key>* .

   If it is a Windows Server 2008 host, run *EqlSetupUtil.exe*.
4. Reboot the system.

   You can run **EqlSetupUtil.exe** to configure the following registry values:

   ```
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk]
   "TimeOutValue"=dword:0000003c
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-
   E325-11CE-BFC1-08002BE10318}\<Instance Number>\Parameters
   ```

   Additionally, each Windows Server 2003 cluster host is required to have the following registry values:

   ```
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msiscdsm
   \PersistentReservation]
   "UsePersistentReservation"=dword:00000001
   "PersistentReservationKey"=hex:<PR key>
   ```

NOTE: <PR Key> is a unique 8-byte binary value that is composed of a 6-byte part that is specific to the cluster and a 2-byte part that is specific to the node. For example if you have a three node cluster you can assign *0xaabbccccbbaa* as the cluster specific part. The nodes can then have the following PR keys:

- Node 1: 0xaabbccccbbaa0001
- Node 2: 0xaabbccccbbaa0002
- Node 3: 0xaabbccccbbaa0003

Configuration Overview Of Shared Storage Arrays

This section contains the following topics:

- Running the Group Manager GUI.
- Creating Volumes.

- Creating Access Control Records.
- Connecting Hosts to Volumes.
- Advanced Storage Features.

Running The Group Manager GUI

You can use the Group Manager graphical user interface (GUI) to configure the storage array(s) and perform other group administration tasks using one of the following methods:

- Use a Web browser through a standard web connection using HTTP (port 80).
- Install the GUI on a local system and run it as a standalone application.

To run the Group Manager GUI on a web browser:

1. Specify the following group IP address in a web browser window **http://group_ip_address**.
   Where *group_ip_address* refers to the IP address that you have configured for the group.
   When you connect to the group, the login dialog box is displayed.
2. Enter a group administration account name.
   You can use the default **grpadmin** account and password you set when creating the group if no other accounts have been set up.

Group Manager GUI Components

The Group Manager GUI enables you to manage various group components, which you access by clicking and expanding objects in the tree structure in the far left panel:

- **Group Configuration** — Modifies the group configuration and set up accounts, event notification, network services, authentication, and SNMP.
- **Group Monitoring** — Monitors iSCSI connections to the group, snapshot and replication schedules, volume replication configurations and activity, administrative sessions and login history, and in-progress member and volume move operations.
- **Events** — Displays events in the group.
- **Storage Pools** — Creates and manages pools in the group.
- **Members** — Monitors and manages group members, including configuring network interfaces.
- **Volumes** — Monitors and manages volumes, snapshots, replicas, and schedules.
- **Volume Collections** — Creates and manages collections of volumes. Organizing multiple, related volumes into a collection enables you to create snapshots or replicas of the volumes in a single operation or schedule.
- **Replication Partners** — Monitors and manages replication partners.

Creating Volumes

To access storage in a PS Series group, you must create one or more storage pools and then allocate portions of the storage pool(s) to volumes. Each volume is assigned a size, storage pool, and access controls. Volumes are seen on the network as iSCSI targets. Only hosts with an iSCSI initiator and the correct access credentials can access a volume. The group automatically generates an iSCSI target name for each volume. This is the name that iSCSI initiators use to access the volume.

To create a volume:

1. Click **Volumes** and **Create volume**.
   The Create Volume-General Settings dialog box is displayed. You can specify information in the following fields:
   - **Volume name** —Unique name, up to 64 alphanumeric characters (including periods, hyphens, and colons), used to identify the volume for administrative purposes. The volume name is displayed at the end of the

iSCSI target name that is generated for the volume. Host access to the volume is always through the iSCSI target name, not the volume name.

- **Description** — The volume description is optional.
- **Storage pool** — All volume data is restricted to the members that make up the pool. By default, the volume is assigned to the default pool. If multiple pools exist, you can assign the volume to a different pool.

2. Click **Next**.

   The **Create Volume – Space Reserve** dialog box is displayed. Specify information in the following fields:

   - **Volume size** — This is the reported size of the volume as seen by iSCSI initiators. The minimum volume size is 15 MB. In addition, volume sizes are rounded up to the next multiple of 15.
   - **Thin provisioned volume** — Select this check box to enable thin provisioning on the volume. When selected, slider bars appear in the Reported volume size panel. Use them to modify the following default thin provisioning values:
     * **Minimum volume reserve** — This is the minimum amount of space to allocate to the volume. As the volume is used, more space is allocated to the volume, and the volume reserve is increased. The default is 10% of the volume size.
     * **In-use space warning value** — When in-use space reaches this value, as a percentage of the volume size, a warning event message is generated. The warning informs you that volume space is being used, enabling you to make adjustments, as needed. The default is the group-wide volume setting.
     * **Maximum in-use space value** — When the in-use space reaches this value, as a percentage of the volume size, the volume is set offline. The default is the group-wide volume setting.
   - **Snapshot reserve** — If you want to create snapshots of the volume, specify the amount of pool space to reserve for snapshots, as a percentage of the volume reserve.

3. Click **Next**.

   The **Create Volume – iSCSI Access Policy** dialog box is displayed, which enables you to create an access control record for the volume.

Creating Access Control Records

Access control records are used to restrict volume access to hosts that supply a CHAP user name and password that is recognized or that match an IP address or iSCSI initiator name (or any combination of the three).

To create an access control record that applies to the volume and its snapshots:

1. In the **Create Volume – iSCSI Access Policy** dialog box, click **Restricted access** and one or more of the following:

   - **Authenticate using CHAP user name** — Restricts access to hosts that supply the specified CHAP user name and the associated password. The user name must match a local CHAP account or an account on an external RADIUS server.
   - **Limit access by IP address** — Restricts access to hosts with the specified initiator IP address (for example, 12.16.22.123). Use asterisks for "wildcards," if desired (for example, 12.16.*.*). An asterisk can replace an entire octet, but not a digit within an octet.
   - **Limit access to iSCSI initiator name** — Restricts access to hosts with the specified iSCSI initiator.

NOTE: When using IP addresses or iSCSI initiator names to restrict access, ensure to create an access control record for each IP address or iSCSI initiator name presented by an authorized host. Additional records can be added if you do not want to create an access control record at this time, select **No access**. No host is allowed access to the volume until you create a record.

2. Select the **Enable shared access to the iSCSI target from multiple initiators** check box.
3. After specifying the access information, click **Next** to display the **Create Volume - Summary** dialog box.
4. Click **Finish** to create the volume.
5. Verify that the volume is enabled for shared access by multiple initiators:

   - Right click on the volume that has just been created, and select **Modify Volume Settings**.

- Select the **Advanced** tab.
- Ensure that the **Enable shared access to the iSCSI target from multiple initiators** check box is selected.

Connecting Hosts To Volumes

This section discusses how to make the proper connection to a PS Series SAN including adding the Target Portal and connecting to volumes from the host. Using the Microsoft iSCSI Initiator Service, add a Target Portal using the PS Series group IP address if it is not present. This allows the host to discover available targets. This process is performed in the **Discovery** area of the initiator properties window.

A volume is seen on the network as an iSCSI target, which can only be accessed by an iSCSI initiator installed on a host.

To log into a volume or target:

1. Under **Targets**, select the volume you want to connect.
2. Click **Log On**.
3. Select the **Enable multi-path** check box in the Microsoft initiator when logging into your target.
4. Select the **Automatically restore this connection when the system boots** check box to make the connections persistent.
5. Click **Advanced**.
   a) In the **Local Adapter** drop box, select **Microsoft iSCSI Initiator**.
   b) In the **Source IP**drop box, select the IP of the appropriate iSCSI NIC.
   c) In the **Target Portal**drop box, select the IP of the PS group.
   d) If you use CHAP as a discovery method, add the Target secret to complete the connection.
6. Repeat step 2 through step 5 using the IP of the other interface that you selected in step 5b.

   After you have made your initial connection, the MPIO DSM connection manager creates all the appropriate connections, and replaces any original connections if necessary. For instance, two NICs and three arrays would result in six connections per volume. After making your initial connection, allow a minute or two for the DSM to communicate with the array group and get sufficient information to create the multiple connections.

   After the initiator logs in to the iSCSI target, the volume is seen by the host as a normal disk that can be formatted using the usual operating system utilities.

Advanced Storage Features

For backup or disaster recovery purposes, you can create volume snapshots, clone a volume, or replicate a volume to a different group. You can create snapshots of the volumes (a snapshot collection) or replicas of the volumes (a replica collection) in a single operation. You can also utilize storage resources using Thin Provisioning.

NOTE: For more information on using Snapshots, Replication, Cloning, Volume Collection, and Thin Provisioning, see the *Group Administration* guide at **equallogic.com**.

This section discusses features provided by the Group Manager GUI. You can also use ASM for backing up and restoring data in the Windows cluster environment. ASM uses Microsoft VSS to provide a framework for creating fast, coordinated copies of application database volumes on your PS Series group, ensuring that the backed-up data is easy to restore and use for recovery.

CAUTION: If you want to mount the volume of a snapshot, clone, or replica using the Group Manager GUI, mount it to a standalone node or a cluster node in a different cluster. Do not mount the snapshot, clone, or replica of a clustered disk to a node in the same cluster because it has the same disk signature as the original clustered disk. Windows detects two disks of the same disk signature and changes the disk signature on one of them. Most of the time, Windows tries to change the disk signature of the snapshot, clone, or replica. If its access type is Read-Only, Windows is unable to change the signature and thus the volume is not mounted. If its access type is Read-Write, Windows is able to change the disk signature. When you try to restore the disk later, the cluster's physical resource fails due to a different disk signature. Although it is rare, under some conditions, Windows can change the disk signature on the original disk because it misidentifies the snapshot, clone, or replica as the cluster disk. That situation may result in data loss or an inaccessible snapshot, clone, or replica.

NOTE: For more information on using ASM in the cluster, see the *Host Integration Tools EqualLogic Auto-Snapshot Manager/Microsoft Edition User Guide* at **equallogic.com**.

NOTE: You can use ASM to mount a snapshot, clone, or replica to the same node or another node in the same cluster. VSS changes the disk signature of the snapshot, clone, or replica before mounting it.

Snapshots

A snapshot is a point-in-time copy of volume data that can protect against mistakes, viruses, or database corruption. Snapshot creation does not disrupt access to the volume. Snapshots appear on the network as iSCSI targets and can be set online and accessed by hosts with iSCSI initiators. You can recover volume data by restoring a volume from a snapshot or by cloning a snapshot, which creates a new volume.

Creating Snapshots

To create a snapshot of the current time:

1. Click **Volumes** → **volume_name** → **Create snapshot.**

   The **Create Snapshot** dialog box is displayed.
2. You can specify the following information in the **Create Snapshot** dialog box:
   - Optional snapshot description.
   - Whether you want the snapshot set offline (default) or online.
   - Whether you want the snapshot to be read-write (default) or read-only.
3. Click **OK** to create the snapshot. The snapshot is displayed in the far left panel, under the volume name identified by the date and time when it was created.

Restoring Snapshots

To restore a volume from a snapshot:

1. Use Cluster Administrator or Failover Cluster Management to bring the cluster resource group containing the volume offline.
2. Use Group Administration to:
   - Bring the volume and the snapshot offline.
   - Select the volume, perform a restore, and select the snapshot to restore the volume from.
   - Bring the volume online.
3. Use Microsoft iSCSI Initiator Service GUI to log back into the volume from each cluster node.
4. Use Cluster Administrator or Failover Cluster Management to bring the cluster group online.

NOTE: Do not use the Group Manager GUI to mount the snapshot of a clustered disk to a node in the same cluster.

Volumes

Cloning a volume creates a new volume with a new name and iSCSI target, having the same size, contents, and Thin Provisioning setting as the original volume. The new volume is located in the same pool as the original volume and is available immediately. Cloning a volume does not affect the original volume, which continues to exist after the cloning operation. A cloned volume consumes 100% of the original volume size from free space in the pool in which the original volume resides. If you want to create snapshots or replicas of the new volume, you require additional pool space.

Cloning Volumes

To clone a volume:

1. Click **Volumes** → **volume_name** → **Clone volume.**

   The **Clone Volume – General Settings** dialog box is displayed.
2. Specify information about the new volume in the following fields:
   - **Volume name** – Unique name, up to 64 alphanumeric characters (including periods, hyphens, and colons), used to identify the volume for administrative purposes. Host access to the volume is always through the iSCSI target name, not the volume name.
   - **Description** – Optional volume description.
3. Click **Next**.

   The **Clone Volume – Space Reserve** dialog box is displayed.
4. In the **Snapshot Reserve** field, specify the amount of space, as a percentage of the volume reserve, to reserve for snapshots of the new volume. The default is the group-wide volume setting.
5. Click **Next**.

   The **Clone Volume – iSCSI Access Policy** dialog box is displayed. This dialog box enables you to create an access control record that restricts host access to the new volume and its snapshots.
6. Select the method of restricting access and specify the required information.
7. Click **Next**.

   The **Clone Volume – Summary** dialog box, which summarizes the volume configuration is displayed.
8. If the configuration is correct, click **Finish** to clone the volume. Click **Back** to make changes, if required.

Restoring Volumes

To restore a volume from a clone:

1. Use Cluster Administrator or Failover Cluster Management to bring the cluster resource group containing the volume offline.
2. Use Microsoft iSCSI Initiator Service GUI from each cluster node to:
   - Log off the volume.
   - Delete the volume from the list of Persistent Targets.
3. Use Group Administration to:
   - Bring the volume offline.
   - Ensure that the clone has Read-Write access and its access control list contains all cluster nodes.
   - Bring the clone online.
4. Use the Microsoft iSCSI Initiator Service GUI to log into the clone from each cluster node.
5. Use the Cluster Administrator or Failover Cluster Management to bring the cluster group online.

NOTE: Do not use the Group Manager GUI to mount the clone of a clustered disk to a node in the same cluster.

Replication

Replication enables you to copy volume data across groups, physically located in the same building or separated by some distance. Replication protects the data from failures ranging from destruction of a volume to a complete site disaster, with no impact on data availability or performance. Similar to a snapshot, a replica represents the contents of a volume at a specific point in time. There must be adequate network bandwidth and full IP routing between the groups.

The volume is located in the primary group and the volume replicas are stored in the secondary group, in the space that is delegated to the primary group. Mutual authentication provides security between the groups. The first replica of a volume is a complete transfer of the volume data from the primary group to the secondary group over the network. For subsequent replicas, only the data that changed since the previous replica is transferred to the secondary group. If you need to transfer a large amount of volume data for the first replication, you can use manual transfer replication.

This enables you to copy the volume data to external media and then load the data from the media to the replica set on the secondary group. After the first data transfer is complete, replication continues, as usual, over the network.

NOTE: To copy the data remotely when you are setting up replication, use the manual transfer utility.

Replicating Volumes

To replicate a volume from one group to another:

1. Configure two groups as replication partners:
   a) Log in to each group.
   b) Configure the other group as a replication partner, and delegate space to the partner.
   c) For each group, specify the partner's name, partner's group IP address, and reciprocal passwords for mutual authentication.
2. Configure replication on the volume:
   a) Log in to the primary group and configure replication on the volume.
   b) Specify the following information for each volume:
      * Partner that stores the replicas (secondary group).
      * Replica reserve size on the secondary group.
      * Local replication reserve size on the primary group and whether to enable the borrow free space option.
      * Whether the first replication occurs over the network or by using manual transfer replication.
      * Whether to keep the failback snapshot. You require more local replication reserve if you keep the failback snapshot.
3. Start the replication:

   Either create a replica or set up a schedule to create replicas on a regular basis.
4. Check that the replication completes:

   Periodically check the replication space utilization and make modifications as needed.

   To recover volume data from replicas in the secondary group, you can clone an individual replica to create a new volume. You can also use failback functionality to temporarily host a volume from the secondary group for backup purposes or if the primary group is unavailable due to failure or maintenance. Later, you can failback to the primary group and return to the original replication configuration, in some cases, by replicating only the volume changes that occurred while the volume was hosted on the secondary group. You can also use failback functionality to permanently switch partner roles.

Volume Collections

NOTE: Do not use the Group Manager GUI to mount the clone of a clustered disk to a node in the same cluster.

A volume collection consists of one or more volumes from any pool and simplifies the creation of snapshots and replicas. Volume collections are useful when you have multiple, related volumes. In a single operation, you can create snapshots of the volumes (a snapshot collection) or replicas of the volumes (a replica collection).

Creating Volume Collections

To create a volume collection:

1. Click **Volume Collections** → **Create volume collection**.
   The **Create Volume Collection – General** window is displayed.
2. Specify a name for the collection and an optional description.
3. Click **Next**.
   The **Create Volume Collection – Components** window is displayed.
4. Select up to eight volumes for a collection. A volume collection can contain volumes from different pools.
5. Click **Next**.
   The **Create Volume Collection – Summary** window is displayed.
6. If the configuration is correct, click **Finish** to create the volume collection.
7. To make changes, click **Back**.
   After creating a volume collection, you can create snapshots or replicas.

Thin Provisioning

You can use thin provisioning technology to provision the storage more efficiently, while still meeting application and user storage needs. A thin-provisioned volume is initially allocated only a portion of the volume size. As data is written to the volume, more space is automatically allocated (if available) from the free pool, and the volume reserve increases up to the user-defined limit. If space is not available, the auto-grow operation fails. If in-use space, typically the volume size, consumes all the volume reserve, the volume is set offline. Thin provisioning is not always appropriate or desirable in an IT environment. It is most effectively used when you know how a volume grows over time, the growth is predictable, and users do not need immediate, guaranteed access to the full volume size. Regular event messages are generated as space is used, giving the administrator the opportunity to make adjustments, as needed. With thin-provisioned volumes, you can utilize storage resources more efficiently, while eliminating the need to perform difficult resize operations on the host.

Installation And Configuration Of A Failover Cluster

You can configure the operating system services on your Failover Cluster, after you have established the private and public networks and have assigned the shared disks from the storage array(s) to the cluster nodes. The procedures to configure the Failover Cluster are different and depends on the Windows Server operating system you use.

For more information on deploying your cluster with Windows Server 2003 operating systems, see the *Dell Failover Clusters with Microsoft Windows Server 2003 Installation and Troubleshooting Guide* at **support.dell.com/manuals**.

For more information on deploying your cluster with Windows Server 2008 operating systems, see the *Dell Failover Clusters with Microsoft Windows Server 2008 Installation and Troubleshooting Guide* at **support.dell.com/manuals**.

4

Troubleshooting

The following section describes general cluster problems you may encounter and the probable causes and solutions for each problem.

Problem	Probable Cause	Corrective Action
The nodes cannot access the storage system, or the cluster software is not functioning with the storage system.	The storage system is not cabled properly to the nodes or the cabling between the storage components is incorrect.	Ensure that the cables are connected properly from the node to the storage system. For more information, see Cabling Your Cluster for Public and Private Networks.
	One of the cables is faulty.	Replace the faulty cable.
	Volumes are not assigned to the hosts.	Verify that all volumes are assigned to the hosts.
One of the nodes takes a long time to join the cluster. Or One of the nodes fail to join the cluster.	The node-to-node network has failed due to a cabling or hardware failure.	• Check the network cabling and verify that the multi-initiator check box is selected. • Ensure that the node-to-node interconnection and the public network are connected to the correct NICs.
	Long delays in node-to-node communications may be normal.	• Verify that the nodes can communicate with each other by running the **ping** command from each node to the other node. • Try both the host name and IP address when using the ping command.
	One or more nodes may have the Internet Connection Firewall enabled, blocking Remote Procedure Call (RPC) communications between the nodes.	• Configure the Internet Connection Firewall to allow communications that are required by the Microsoft Cluster Service (MSCS) and the clustered applications or services. • For more information, see the article KB883398 at **support.microsoft.com**.
Attempts to connect to a cluster using Cluster Administrator fail.	• The Cluster Service has not been started. • A cluster has not been formed on the system.	• Verify that the Cluster Service is running and that a cluster has been formed.

Problem	Probable Cause	Corrective Action

	• The system has just been booted and services are still starting.	• Use the Event Viewer and look for the following events logged by the Cluster Service:
		`Microsoft Cluster Service successfully formed a cluster on this node.`
		Or
		`Microsoft Cluster Service successfully joined the cluster.`
		• If these events do not appear in Event Viewer, see the *Microsoft Cluster Service Administrator's Guide* for instructions on setting up the cluster on your system and starting the Cluster Service.

	The cluster network name is not responding on the network because the Internet Connection Firewall is enabled on one or more nodes.	Configure the Internet Connection Firewall to allow communications that are required by MSCS and the clustered applications or services. For more information, see the article KB883398 at **support.microsoft.com**.
You are prompted to configure one network instead of two during MSCS installation.	The TCP/IP configuration is incorrect.	The node-to-node network and public network must be assigned static IP addresses on different subnets.
	The private (point-to-point) network is disconnected.	Ensure that all systems are powered on so that the NICs in the private network are available.
Using Microsoft Windows NT 4.0 to remotely administer a Windows Server 2003 cluster generates error messages.	This is a known issue. Some resources in Windows Server 2003 are not supported in Windows NT 4.0.	It is strongly recommended that you use Windows XP Professional or Windows Server 2003 for remote administration of a cluster running Windows Server 2003.
Unable to add a node to the cluster.	The new node cannot access the shared disks. The shared disks are enumerated by the operating system differently on the cluster nodes.	Using Windows Disk Administration ensure that the new cluster node can enumerate the cluster disks. If the disks do not appear in Disk Administration: 1. Check all cable connections. 2. Check the volumes assignments. 3. Select **Advanced** → **Minimum**.

Problem	Probable Cause	Corrective Action
	One or more nodes may have the Internet Connection Firewall enabled, blocking RPC communications between the nodes.	Configure the Internet Connection Firewall to allow communications that are required by the MSCS and the clustered applications or services. For more information, see the article KB883398 at **support.microsoft.com**.
Unable to use Microsoft iSCSI Initiator to connect to the PS Series array(s) from the second node and the following error message is displayed: `Authorization Failure.`	The **Enable shared access to the iSCSI target from multiple initiators** check box is not selected.	1. In the Group Manager GUI, right click the volume having the connection problem. 2. Select **Modify Volume Settings**. 3. Click the **Advanced** tab and ensure that the volume is enabled for shared access from multiple initiators.
The disks on the shared cluster storage are unreadable or uninitialized in Windows Disk Administration.	• This issue occurs if you stop the Cluster Service. • On systems running Windows Server 2003, this issue occurs if the cluster node does not own the cluster disk.	No action required.
Cluster Services does not operate correctly on a cluster running Windows Server 2003 and with Internet Firewall enabled.	The Windows Internet Connection Firewall is enabled, which may conflict with Cluster Services.	Perform the following steps: 1. On the Windows desktop, right-click **My Computer** and click **Manage**. 2. In the **Computer Management** window, double-click **Services**. 3. In the **Services** window, double-click **Cluster Services**. 4. In the **Cluster Services** window, click the **Recovery** tab. 5. Click the **First Failure** dropdown arrow and select **Restart the Service**. 6. Click the **Second Failure** dropdown arrow and select **Restart the Service**. 7. Click **OK**. For information on how to configure your cluster with the Windows Internet Connection Firewall enabled, see the articles 258469 and 883398 at **support.microsoft.com** and **microsoft.com/technet** respectively.
Public network clients cannot access the applications or services that are provided by the cluster.	One or more nodes may have the Internet Connection Firewall enabled, blocking RPC communications between the nodes.	Configure the Internet Connection Firewall to allow communications that are required by the MSCS and the clustered applications or services. For more information, see the article KB883398 at **support.microsoft.com.**

Problem	Probable Cause	Corrective Action
The storage array firmware upgrade process using Telnet, exits without allowing you to enter `y` to the following message: `Do you want to proceed (y/n)[n]:`	The Telnet program sends an extra line after you press <Enter>	User serial connection for the array firmware upgrade. To clear the extra linefeed in Windows Telnet: 1. Enter **^]**(control, right bracket). 2. In the Microsoft Telnet prompt, type `unset crlf`. 3. Press <Enter> to return to Telnet.
While running the Cluster Validation Wizard, the Validate IP Configuration test detects that two iSCSI NICs are on the same subnet and a warning is displayed.	The two iSCSI NICs are configured in the same subnet by design.	No action required.

5

Cluster Data Form

You can attach the following form in a convenient location near each cluster node or rack to record information about the cluster. Use the form when you call for technical support.

Table 1. Cluster Configuration Information

Cluster Information	Cluster Solution
Cluster name and IP address	
Server type	
Installer	
Date installed	
Applications	
Location	
Notes	

Table 2. Cluster Node Configuration Information

Node Name	Service Tag Number	Public IP Address	Private IP Address

Table 3. Additional Network Information

Additional Networks

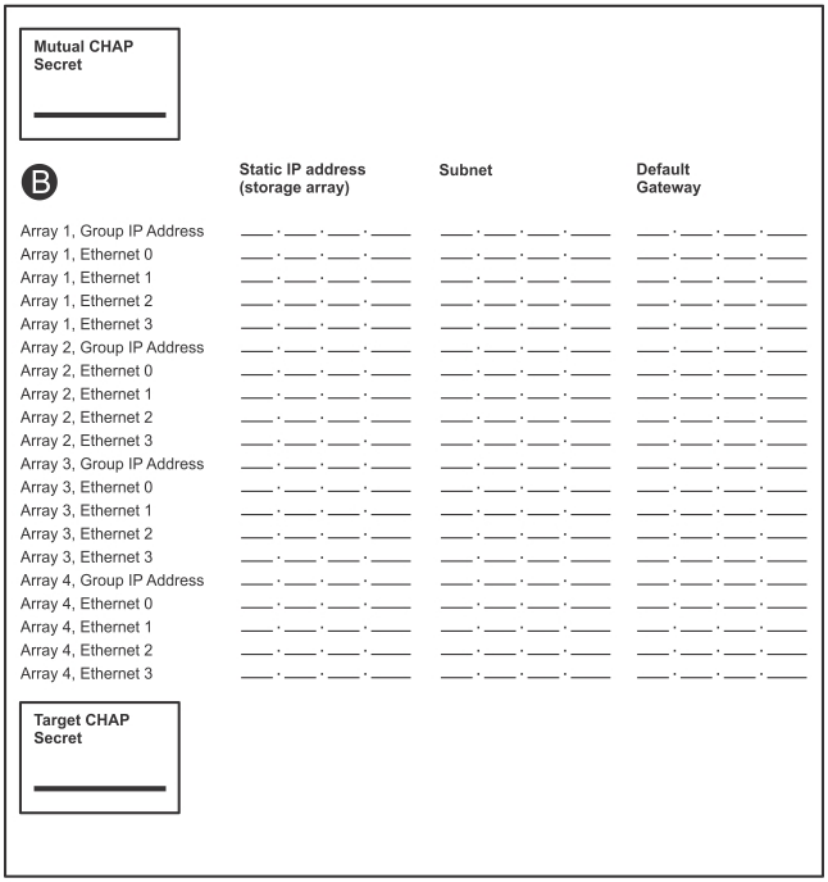
Table 4. Storage Array Configuration Information

Array	Array Service Tag	Group IP Address	Group Name	Member Name	Volume Names
1					
2					
3					

iSCSI Configuration Worksheet

If you need additonal space for additional servers or storage arrays, use an additional sheet.

Ⓐ	Static IP address (host server)	Subnet	Default Gateway
Server 1, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 1, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 2, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 2, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 3, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 3, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 4, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 4, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 5, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 5, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 6, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 6, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 7, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 7, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 8, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 8, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 9, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 9, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 10, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 10, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 11, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 11, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 12, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 12, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 13, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 13, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 14, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 14, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 15, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 15, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 16, iSCSI NIC port 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server 16, iSCSI NIC port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___


Mutual CHAP Secret
B
Static IP address (storage array)
Subnet
Default Gateway
Array 1, Group IP Address
Array 1, Ethernet 0
Array 1, Ethernet 1
Array 1, Ethernet 2
Array 1, Ethernet 3
Array 2, Group IP Address
Array 2, Ethernet 0
Array 2, Ethernet 1
Array 2, Ethernet 2
Array 2, Ethernet 3
Array 3, Group IP Address
Array 3, Ethernet 0
Array 3, Ethernet 1
Array 3, Ethernet 2
Array 3, Ethernet 3
Array 4, Group IP Address
Array 4, Ethernet 0
Array 4, Ethernet 1
Array 4, Ethernet 2
Array 4, Ethernet 3
Target CHAP Secret